PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-302034

(43)Date of publication of application : 13.11.1998

(51)Int.Cl. G06K 17/00
G06T 7/00
G06K 19/10

(21)Application number : 09-107101

(22)Date of filing : 24.04.1997

(71)Applicant : N T T DATA:KK

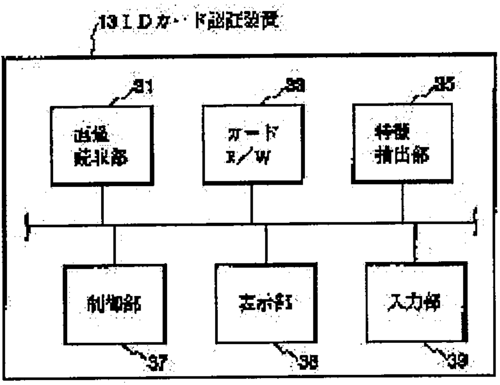
(72)Inventor : ARAKAWA HIROKI
IWAMOTO HIROKI

(54) AUTHENTICATION SYSTEM, CARD ISSUING DEVICE, AUTHENTICATION DEVICE, CARD FOR AUTHENTICATION AND AUTHENTICATION METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To detect a forged unauthorized card by storing feature data in the magnetic storage part of a card for authentication and collating data read from the magnetic storage part with the data generated by extracting features from image information.

SOLUTION: The image read part 31 of an ID card authentication device 13 is constituted of an image scanner or the like for instance, reads a photograph (image) stuck to the photograph sticking part of an ID card and obtains image data. A card reader/writer 33 writes the data to a magnetic stripe or reads the data stored on the magnetic stripe. Also, a feature extraction part 35 extracts the feature data for specifying the image data from the obtained image data. Then, at the time of authenticating the ID card, a control part 37 compares the data stored on the magnetic stripe with the feature data extracted from the photograph stuck to the photograph sticking part of the ID card of an authentication object and checks the propriety of the ID card.



Japanese Patent Application Laid-Open No. 10-302034

Laid-Opened Date: November 13, 1998

Application Number: 9-107101

Filing Date: April 24, 1997

Applicant: NTT DATA KK

Inventor: HIROKI ARAKAWA

Inventor: HIROKI IWAMOTO

---

(54) [Title of the Invention]

AUTHENTICATION SYSTEM, CARD ISSUING APPARATUS, AUTHENTICATION APPARATUS, AUTHENTICATION CARD, AND AUTHENTICATION METHOD

(57) [Abstract]

[Problem to be solved]

To provide a low-priced, simple ID card that can be hardly forged and an authentication system and method that use the ID card.

[Solution]

The ID card has a photograph attaching part to which a user's photograph is attached, and a magnetic stripe. In issuing the ID card, an ID card authentication apparatus 13 scans an image of a photograph that is attached to the ID card, and stores feature data that is generated by extracting a feature in a magnetic stripe. In authenticating the ID card, the ID card authentication apparatus 13 scans the

photograph that is attached to the ID card, generates the feature data by performing feature extraction, and compares it with the feature data that is previously stored in the magnetic stripe. If the compared feature data match, the ID card authentication apparatus 13 determines that the ID card to be authenticated is a normal card. If the compared feature data do not match, the ID card authentication apparatus 13 performs detection processing of a fraudulent card.

[Claims for the Patent]

[Claim 1]

An authentication system comprising an authentication card and an authentication apparatus, wherein said authentication card has image information for identifying a user displayed thereon and comprises a storage unit and said authentication apparatus processes the authentication card; characterized in that said authentication apparatus comprises:

card issuing means comprising scanning means for scanning said image information that is displayed on said authentication card; feature extracting means for extracting a feature from said image information that is scanned by said scanning means and generating feature data; and writing means for writing said feature data in said storage unit; and

authenticating means comprising generating means for scanning said image information that is displayed on said authentication card by said scanning means and generating feature data by said feature extracting means in authentication; reading means for reading said feature data that is written in said storage unit of said authentication card by said writing means; determining means for determining whether said feature data that is read from said reading means matches said feature data that is generated by said generating means or not; and means for reporting detection of a fraudulent card, if it is determined that said feature data that is read from said reading means does not match said feature data that is generated by said generating means.

[Claim 2]

A card issuing apparatus in an authentication system wherein said authentication system authenticates a user by using an authentication card that has image information for identifying a user displayed thereon and comprises a storage unit; characterized by comprising:

scanning means for scanning said image information that is previously displayed on said authentication card;

feature extracting means for extracting a feature from said image information that is scanned by said scanning means and generating feature data; and

writing means for writing said feature data in said storage unit.

[Claim 3]

An authentication apparatus that authenticates an authentication card that has image information for identifying a user displayed thereon and comprises a storage unit that stores feature data that is generated by extracting a feature from the image information; characterized by comprising:

scanning means for scanning said image information that is displayed on said authentication card;

feature extracting means for extracting a feature from said image information that is scanned by said scanning means and generating feature data;

reading means for reading said feature data that is written in said storage unit of said authentication card;

determining means for determining whether said feature data that is read by said reading means matches said feature data that is generated by said feature extracting means or not; and

means for reporting detection of a fraudulent card, if it is determined that said feature data that is read by said reading means does not match said feature data that is generated by said feature extracting means.

[Claim 4]

An authentication card that is used in an authentication system that authenticates a user; characterized by comprising:

a display area for displaying image information for identifying a user; and

a storage area for storing feature data that is generated by extracting a feature from said image information that is displayed on said display area.

[Claim 5]

An authentication method that authenticates a user by using an authentication card that has image information for identifying the user displayed thereon and comprises a storage unit; characterized by comprising:

a scanning step of scanning said image information that is previously displayed on said authentication card;

a feature extracting step of extracting a feature from said scanned image information and generating feature data; and

a storing step of storing said feature data that is generated at said feature extracting step in said storage unit of said authentication card.

[Claim 6]

An authentication method that authenticates a user by using an authentication card that has image information for identifying the user displayed thereon and comprises a storage unit that stores feature data that is generated by extracting a feature from the image information; characterized by comprising:

a scanning step of scanning said image information that is previously displayed on said authentication card;

a feature extracting step of extracting a feature from said image information that is scanned by said scanning step and generating feature data;

a reading step of reading said feature data that is previously stored in said storage unit of said authentication card;

a determining step of determining whether said feature data that is read by said reading step matches said feature data that is generated by said feature extracting step or not; and

a step of reporting detection of a fraudulent card, if it is determined that said feature data that is read by said reading step does not match said feature data that is generated by said feature extracting step.

[Detailed Description of the Invention]

[0001]

[Field of the Invention]

The present invention relates to an authentication system for authenticating a user.

[0002]

[Conventional Art]

In an authentication system that involves an ID card or the like, to which a user's photograph is attached, it is required to confirm that the attached photograph is not an fraudulently replaced one. In view of that requirement, for example, authentication systems that store image data of the attached photograph in the ID card and perform authentication by comparing the attached photograph and the image data have been proposed.

[0003]

[Problems to be Solved by the Invention]

As one of the systems, a system that uses image data of the attached photograph, for example, as data to be stored in the ID card is proposed. In that case, an amount of the data is so large that a storage medium with a small storage capacity like a magnetic stripe type is incapable and IC (Integrated Circuit) memory with a large storage capacity is required.

[0004]

In view of that requirement, a system for storing compressed image data of the photograph in the ID card is also proposed where the image data of the photograph is compressed, and accordingly, the amount of the data is reduced. That case, however, has a problem in that it is impracticable to confirm that the expanded data, which is the compressed data that is previously stored in the card, matches the image data of the attached photograph. This is because that when the compressed data is expanded, it may not completely match the data before the compression.

[0005]

In order to address that problem, in Japanese Patent Application Laid-Open Publication No. 8-129634, for example, a system that scans the attached photograph, compresses the photograph in the same manner as that used for the compressed data that is previously stored in the card, and then expands the photograph, and compares the resulted data and the expanded data that is compressed and stored in the card in authentication is proposed. That case, however, the data that is stored in the card needs to be expanded and the image data of the photograph that is attached to the card needs to be compressed and then expanded, which causes a problem of slow response.

[0006]

The present invention has been made in view of the abovementioned circumstances and intends to provide an ID card that is priced low with a simple configuration but is hardly forged; an authentication system, apparatus and method that use the ID card. Another object of the present invention is to provide a card issuing apparatus and an authentication card that are preferably used for them.

[0007]

[Means for Solving the Problems]

In order to achieve the abovementioned objects, the authentication system according to the first aspect of the present invention is an authentication system comprising an authentication card and an authentication apparatus, wherein the authentication card has image information for identifying a user displayed thereon and comprises a storage unit and the authentication apparatus processes the authentication card; the authentication apparatus comprising: card issuing means comprising scanning means for scanning the image information that is displayed on the authentication card; feature extracting means for extracting a feature from the image information that is scanned by the scanning means and generating feature data; and writing means for writing the feature data in the storage unit; and authenticating means comprising generating means for scanning the image information that is displayed on the authentication card by the scanning means and generating feature data by the feature extracting means in authentication; reading means for reading the feature data that is written in the storage unit of the authentication card by the writing means; determining means for determining whether the feature data that is read from the reading means matches the feature data that is generated by the generating means or not; and means for reporting detection of a fraudulent card, if it is determined that the feature data that is read from the reading means does not match the feature data that is generated by the generating means.

[0008]

According to the configuration, the feature data that is generated by extracting the feature from the image information for identifying the user is stored in the storage unit, and the data that is read from the storage unit is compared with the data that is generated by extracting a feature from the image information in authentication. That enables the fraudulent card that is forged by illegally changing the image information such as by replacing the attached photograph with another one to be detected. In addition, as only the feature is extracted from the image information, the data that is to be stored in the card results in a small amount. That enables the authentication card to be implemented by a magnetic storage medium or the like that is priced low with a simple configuration.

[0009]

The card issuing apparatus according to the second aspect of the present invention is a card issuing apparatus in an authentication system wherein the authentication system authenticates a user by using an authentication card that has image information for identifying a user displayed thereon and comprises a storage unit comprising: scanning means for scanning the image information that is previously displayed on the authentication card; feature extracting means for extracting a feature from the image information that is scanned by the scanning means and generating feature data; and writing means for writing the feature data in the storage unit.

[0010]

According to the configuration, the feature data that is generated by extracting the feature from the image information for identifying the user is stored in the storage unit as data for comparing in the authentication. That can prevent a card from being forged that is conducted by illegally changing the image information such as by replacing the attached photograph with another one. In addition, as only the feature is extracted from the image information, the data that is to be stored in the card results in a small amount. That enables the authentication card to be implemented by a magnetic storage medium or the like that is priced low with a simple configuration.

[0011]

The authentication apparatus according to the third aspect of the present invention is an authentication apparatus that authenticates an authentication card that has image information for identifying a user displayed thereon and comprises a storage unit that stores feature data that is generated by extracting a feature from the image information; comprising: scanning means for scanning the image information that is previously displayed on the authentication card; feature extracting means for extracting a feature from the image information that is scanned by the scanning means and generating feature data; reading means for reading the feature data that is written in the storage unit of the authentication card; determining means for determining whether the feature data that is read by the reading means matches the feature data that is generated by the generating means or not; and means for reporting detection of a fraudulent card, if it is determined that the feature data that is read by the reading means does not match the feature data that is generated by the generating means.

[0012]

According to the configuration, the data that is generated by previously extracting the feature that is read from the storage unit is compared with the data that is generated by extracting the feature from the image information in authenticating the card. That enables a fraudulent card, which is forged by illegally changing the image information such as by replacing the attached photograph with another one, to be detected.

[0013]

The authentication card according to the fourth aspect of the present invention is an authentication card that is used in an authentication system that authenticates a user comprising: a display area for displaying image information for identifying a user; and a storage area for storing feature data that is generated by extracting a feature from the image information that is displayed on the display area.

[0014]

According to the configuration, the authentication card has the storage area for storing the feature data that is generated by extracting the feature from the image information for identifying the user as data for comparing in the authentication. That can prevent a card from being forged that is conducted by illegally changing the image information such as by replacing the attached photograph with another one. In addition, as only the feature is extracted from the image information, the data that is to be stored in the card results in a small amount. That enables the authentication card to be implemented by a storage medium or the like that has a simple configuration.

[0015]

The authentication method according to the fifth aspect of the present invention is an authentication method that authenticates a user by using an authentication card that has image information for identifying the user displayed thereon and comprises a storage unit comprising: a scanning step of scanning the image information that is displayed on the authentication card; a feature extracting step of extracting a feature from the scanned image information and generating feature data; and a storing step of storing the feature data that is generated at the feature extracting step in the storage unit of the authentication card.

[0016]

According to the configuration, the feature data that is generated by extracting the feature from the image information for identifying the user is stored in the storage area of the authentication card as data for comparing in the authentication. That can prevent a card from being forged that is conducted by illegally changing the image information such as by replacing the attached photograph with another one. In addition, as only the feature is extracted from the image information, the data that is to be stored in the card results in a small amount. That enables the authentication card to be implemented by a storage medium or the like that is priced low with a simple configuration.

[0017]

The authentication method according to the sixth aspect of the present invention is an authentication method that authenticates a user by using an authentication card that has image information for identifying the user displayed thereon and comprises a storage unit that stores feature data that is generated by extracting a feature from the image information comprising: a scanning step of scanning the image information that is previously displayed on the authentication card; a feature extracting step of extracting a feature from the image information that is scanned by the scanning step and generating feature data; a reading step of reading the feature data that is previously stored in the storage unit of the authentication card; a determining step of determining whether the feature data that is read by the reading step matches the feature data that is generated by the feature extracting step or not; and a step of reporting detection of a fraudulent card, if it is determined that the feature data that is read by the reading step does not match the feature data that is generated by the feature extracting step.

[0018]

According to the configuration, the data that is generated by previously extracting the feature that is read from the storage unit is compared with the data that is generated by extracting the feature from the image information in authenticating the card. That enables a fraudulent card, which is forged by illegally changing the image information such as by replacing the attached photograph with another one, to be detected.

[0019]

[Embodiments of the Invention]

An authentication system according to an embodiment of the present invention will be described below with reference to the drawings. The authentication system includes an ID card and an ID card authentication apparatus. Schematic diagrams of an ID card 11 and an ID card authentication apparatus

13 are shown in Figure 1 and Figure 2, respectively. As shown in Figure 1, the ID card 11 has a photograph attaching part 21, to which a card owner's photograph is attached; and a magnetic stripe 23, which is a magnetic storage medium in the shape of a tape. As shown in Figure 2, the ID card authentication apparatus 13 includes an image scanning part 31, a card reader/writer (card R/W) 33, a feature extracting part 35, a controlling part 37, a displaying part 38, and an inputting part 39.

[0020]

The image scanning part 31, which includes an image scanner or the like, for example, scans a photograph (image) that is attached to the photograph attaching part 21 of the ID card 11 and acquires image data. The card reader/writer 33 writes data in the magnetic stripe 23, or reads data that is stored in the magnetic stripe 23. The feature extracting part 35 extracts feature data for identifying the image data, which is acquired by the image scanning part 31, from the image data. The extracting method will be described later.

[0021]

The controlling part 37 checks validity of the ID card 11 by comparing the data that is stored in the magnetic stripe 23 and the feature data that is extracted from the photograph that is attached to the photograph attaching part 21 of the ID card 11 to be authenticated, in authenticating the ID card 11. Further, the controlling part 37 controls over the ID card authentication apparatus 13. The displaying part 38 displays a result and the like of the authentication of the ID card 11. The inputting part 39 is for a user or an administrator to input an instruction.

[0022]

The system performs issuance of the ID card 11 and authentication of the ID card 11. The processing of them will be described below. First, in order to issue the ID card 11, the user or the administrator attaches a photograph of a person who is to own the card to the photograph attaching part 21 of the ID card 11, sets the card to the image scanning part 31 of the ID card authentication apparatus 13, and inputs an instruction to issue a card from the inputting part 39. In response to the input of the instruction to issue the card, the controlling part 37 of the ID card authentication apparatus 13 starts card issuance processing. The card issuance processing will be described below with reference to the flowchart of Figure 3.

[0023]

First, the controlling part 37 of the ID card authentication apparatus 13 instructs the image scanning part 31 to scan the image of the photograph that is attached to the photograph attaching part 21 of the ID card 11. In response to the instruction, the image scanning part 31 scans the image of the photograph that is attached to the photograph attaching part 21 of the ID card 11 and generates the image data such as bitmap data or the like, for example, by performing predetermined conversion processing (steps S1 and S2).

[0024]

Next, the controlling part 37 instructs the feature extracting part 35 to extract a feature part from the image data and generate the feature data. In response to the instruction, the feature extracting part 35 performs extraction processing for the feature part (feature extraction processing) on the bitmap data that is generated by the image scanning part 31 and generates the feature data (step S3). The feature extraction processing is the processing for reducing the amount of data by extracting only the information on a predetermined feature part from the large amount of bitmap data. An example of the feature extraction processing will be described with reference to Figure 4.

[0025]

First, the feature extracting part 35 identifies locations of the left eye, the right eye and the mouth (points A, B and C in Figure 4) on the image (bitmap data) of the user that is acquired by the image scanning part 31, and generates first feature data by intervals between the locations, i.e., distances AB, BC, and CA. Next, the feature extracting part 35 identifies the inner ends of the eyebrows (points D and F) and the outer ends of the eyebrows (points E and G), and generates second feature data by the locations. Next, the feature extracting part 35 identifies both ends of the eyes (points H, I, J and K), and generates third feature data by the locations. As a result, the feature extracting part 35 generates feature extraction data by the first, the second and the third feature data, for example.

[0026]

Next, the feature extracting part 35 sends a report that the feature data has been generated to the controlling part 37. In response to the report, the controlling part 37 displays a message to request to set the ID card 11 to the card R/W 33 on the displaying part 38. The user or the administrator sets the ID card 11 to the card R/W 33. In addition, the controlling part 37 instructs the card R/W 33 to write the feature data that is generated by feature extracting part 35 to the ID card 11. In response to the instruction from the controlling part 37, the card R/W 33 writes the feature data to the magnetic stripe 23 of the ID card 11 that is set the card R/W 33 (step S4). Here, the issuance of the ID card 11 whose magnetic stripe 23 stores the feature data that identifies the photograph that is attached to the photograph attaching part 21 has completed.

[0027]

The feature data that has been generated in the abovementioned manner is the data that indicates distances, locations and the like with a quite small amount of data compared with that of conventional image data or data that is made by compressing image data. That enables the ID card to be implemented by a magnetic storage medium or the like that is priced low with a simple configuration.

[0028]

When the user needs to be authenticated, the ID card authentication apparatus 13 authenticates the ID card 11 that is issued by the abovementioned issuance processing by comparing the photograph that is attached to the photograph attaching part 21 of the ID card 11 and the feature data that is stored in the magnetic stripe 23. The authentication processing will be described with reference to Figure 5.

[0029]

First, the user or the administrator sets the ID card 11 to be authenticated to the image scanning part 31 of the ID card authentication apparatus 13, and inputs an instruction to request the authentication of the ID card 11 from the inputting part 39. In response to the input of the instruction, the controlling part 37 instructs the image scanning part 31 to scan the image of the photograph that is attached to the photograph attaching part 21 of the ID card 11. In response to the instruction, the image scanning part 31 scans the image of the photograph that is attached to the photograph attaching part 21 of the ID card 11 and generates bitmap data by performing predetermined conversion processing (steps S11 and S12).

[0030]

Next, the controlling part 37 instructs the feature extracting part 35 to generate the feature data from the generated bitmap data. In response to the instruction, the feature extracting part 35 performs feature extraction processing on the generated bitmap data and generates the feature data (step S13). The feature extraction processing is performed in the same manner as that of the feature extraction processing in the abovementioned card issuance processing.

[0031]

In addition, the controlling part 37 instructs the card R/W 33 to read the feature data that is stored in the magnetic stripe 23 of the ID card 11. In response to the instruction, the card R/W 33 reads the feature data from the magnetic stripe 23 of the ID card 11 (step S14).

[0032]

Next, the controlling part 37 compares the feature data that is acquired from the photograph that is attached to the photograph attaching part 21 of the ID card 11 and the feature data that is read from the magnetic stripe 23, and determines whether they match or not (step S15). If it is determined that they match, the controlling part 37 takes the ID card 11 as a normal card without being tampered, and performs normal processing such as displaying of a message that the ID card 11 is normal (step S16), for example. If it is determined that they do not match, the controlling part 37 takes the ID card 11 as a fraudulent card, and performs error processing such as sounding of the alarm, displaying of an error message and the like (step S17).

[0033]

In that manner, a forged fraudulent ID card can be detected by comparing the photograph that is attached to the photograph attaching part 21 of the ID card 11 and the feature data that is stored in the magnetic stripe 23.

[0034]

In the authentication processing here, only the feature data, which is acquired from the image (for example, codes indicating a distance, a location and the like), is compared with each other instead of comparing a large amount of image data each other as in the conventional art. Therefore, the processing speed here can be faster than that of the conventional art.

[0035]

The ID card in the above description is not limited to the shape of a card and may take any shape as long as it has the photograph attaching part to which the photograph is attached and the magnetic stripe that stores the abovementioned feature data. For example, the present invention can be implemented as an authentication system including a passport that has a photograph attaching part and a magnetic stripe and a passport authentication apparatus that performs issuance and authentication of the passport. That enables the forged fraudulent passport to be detected.

[0036]

The items that are subjected to the feature extraction in the feature extraction processing are not limited to the items that are used in the above description (intervals between the eyes, the nose, and the mouth, the inner ends/ the outer ends of the eyebrows, both ends of the eyes) and may be any items. For example, the feature of the face may be extracted by using color features of the face and the like. The feature extraction data that can identify the user more correctly by weighting each of a plurality of items may be generated. In that case, for example, the feature data for a part whose feature data differs largely among individuals may be heavily weighted and the feature data for a part whose feature data differs little among individuals may be lightly weighted.

[0037]

The object of the feature extraction processing is not limited to a photograph and may be anything as long as it can identify the user. For example, an ID card that includes areas for displaying a fingerprint, a portrait and the like of the user and has the feature extraction data of them written in the magnetic stripe may be used.

[0038]

The ID card authentication apparatus of the present invention can be implemented by using a typical computer system instead of a dedicated system. For example, the ID card authentication apparatus for performing the abovementioned processing can be configured by installing a program for performing the abovementioned operations from a medium (a floppy disk, a CD-ROM or the like) that stores the program to a computer, to which an image scanner and a card reader/writer are connected.

[0039]

The medium for supplying the program to the computer may be a communication medium (a medium that temporary and flexibly saves a program such as a communication line, a communication network, and a communication system). For example, the program may be posted to a BBS (Bulletin Board System) of a communication network so as to be distributed over the network. Then, the abovementioned processing may be performed by activating. the program, and under the control of the OS, executing the program in the same manner as that of the other application program.

[0040]

Alternatively, the operation program may be distributed to the ID card authentication apparatus over the network when the feature extraction processing is performed, and the program may be deleted after the feature extraction processing is done. That can prevent a fraud from breaking the ID card authentication apparatus, depriving the ID card authentication apparatus of the feature extraction program that is stored therein, and forging the ID card 11 by using the program. When the program is distributed over the network as mentioned above, it is preferable to enhance the security.

[0041]

[Advantage of the Invention]

As mentioned above, according to the present invention, the feature data that is generated by extracting the feature from the image information for identifying the user is stored in the magnetic storage unit of the authentication card, and the data that is read from the magnetic storage unit is compared with the data that is generated by extracting the feature from the image information in authentication. That enables the fraudulent card that is forged by illegally changing the image information such as by replacing the attached photograph with another one to be detected. In addition, as only the feature is extracted from the image information, the data that is to be stored in the authentication card results in a small amount. That enables the authentication card to be implemented by a storage medium that is priced low with a simple configuration.

[Brief Description of the Drawings]

[Figure 1]

Figure 1 is a diagram showing a configuration of an ID card of an ID card authentication system according to an embodiment of the present invention;

[Figure 2]

Figure 2 is a diagram showing a configuration of an ID card authentication apparatus of an ID card authentication system according to the embodiment of the present invention;

[Figure 3]

Figure 3 is a flowchart for illustrating card issuance processing;

[Figure 4]

Figure 4 is a diagram for illustrating feature extraction processing; and

[Figure 5]

Figure 5 is a flowchart for illustrating authentication processing.

[Description of Symbols]

11 ID card

13 ID card authentication apparatus

21 photograph attaching part

23 magnetic stripe

31 image scanning part

33 card R/W

35 feature extracting part

37 controlling part

38 displaying part

39 inputting part

Figure 1

11 ID CARD

21 PHOTOGRAPH ATTACHING PART

23 MAGNETIC STRIPE

Figure 2

13 ID CARD AUTHENTICATION APPARATUS

31 IMAGE SCANNING PART

33 CARD R/W

35 FEATURE EXTRACTING PART

37 CONTROLLING PART

38 DISPLAYING PART

39 INPUTTING PART

Figure 3

#1 CARD ISSUANCE PROCESSING

S1 SCAN PHOTOGRAPH THAT IS ATTACHED TO ID CARD

S2 GENERATE BITMAP DATA FROM SCANNED DATA

S3 GENERATE FEATURE DATA

S4 WRITE FEATURE DATA IN MAGNETIC STRIPE

#2 END

Figure 4

#1 OUTER ENDS OF EYEBROWS

#2 INNER ENDS OF EYEBROWS

#3 BOTH ENDS OF EYE

Figure 5

#1 AUTHENTICATION PROCESSING

S11 SCAN IMAGE OF PHOTOGRAPH THAT IS ATTACHED TO ID CARD

S12 GENERATE BITMAP DATA

S13 GENERATE FEATURE DATA

S14 READ FEATURE DATA FROM MAGNETIC STRIPE OF ID CARD

S15 DOES FEATURE DATA THAT IS ACQUIRED FROM ATTACHED PHOTOGRAPH MATCH FEATURE DATA THAT IS STORED IN MAGNETIC STRIPE?

S16 NORMAL PROCESSING

S17 ERROR PROCESSING

#2 END